ORIGINAL

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

UNITED STATES OF AMERICA

v.

CHRISTOPHER ROBERT WEAST (01)

No. 4:14-CR-023-A

GOVERNMENT'S RESPONSE TO WEAST'S MOTION TO SUPPRESS

TO THE HONORABLE JOHN McBRYDE, UNITED STATES DISTRICT JUDGE

The United States Attorney for the Northern District of Texas, by and through the undersigned Assistant United States Attorney, files this response in opposition to Weast's motion to suppress and shows the Court as follows:

Issues

(1) Does the defendant have a reasonable expectation of privacy in computer files that he shares with the public?

(2) Does the defendant have a reasonable expectation of privacy in an IP address that is available to the public or an Internet account that contains information voluntarily provided by the subscriber?

Summary

The defendant has no reasonable expectation of privacy in files that he shares with the public. Second, the defendant has no reasonable expectation of privacy in subscriber information maintained by an internet service provider because there is no legitimate expectation of privacy in information voluntarily turned over to third parties.

Relevant Facts

In June 2012, Fort Worth Police Department Officer Randy Watkins initiated a peer-to-peer file sharing investigation in order to identify individuals in the Fort Worth area who were distributing child pornography files over the Internet. On June 4, 2012, Officer Watkins used a program called Child Protection System (CPS) to obtain a list of IP addresses in the Fort Worth area that had offered to distribute known or suspected child pornography. Officer Watkins identified an IP address, 99.71.201.174, which was offering to share files via the Internet using the Gnutella Network. According to the CPS program, a computer using IP address 99.71.201.174 was offering more than 1,000 files that appeared to be images or videos of known or suspected child pornography.[1]

On the same day, Officer Watkins used ShareazaLE,[2] a file-sharing program to make a direct, single-source connection between Watkins's undercover computer and defendant Weast's computer (subsequently identified), which was using the IP address 99.71.201.174 to make child pornography files available. Thereafter, between June 4, 2012 and June 19, 2012, the defendant's computer shared 66 files of child pornography—all of which were publicly available at the time Officer Watkins downloaded these files. Officer Watkins also noticed in the download log files that the computer sharing files of child pornography had a nickname, "Chris."

[1] The CPS system compares SHA values of images and videos against a database of images and videos known to or suspected of being child pornography. A SHA value is a Secure Hash Algorithm, similar to an electronic fingerprint for files.

[2] Like other publicly available programs, ShareazaLE allows law enforcement to download files from other computers on the same file-sharing network. While this program permits law enforcement to download files entirely from a single source rather than from multiple sources, it does not give law enforcement any greater access to another peer-to-peer user's computer than that available to the rest of the public.

Using another publicly available tool, CentralOps.net, Officer Watkins determined that the IP address 99.71.201.174 was owned by SBC Internet Services. Officer Watkins requested a subpoena through the Tarrant County District Attorney's Office for subscriber information for the Internet account assigned to IP address 99.71.201.174, on June 4, 2012 at 19:21 GMT (the date and time Officer Watkins downloaded child pornography from that IP address.) AT&T responded to the subpoena and provided the name of the account holder, Larry Weast, and the service location assigned to the Internet account, 833 Hallvale Road, White Settlement, Texas. Based on the images that Officer Watkins downloaded and the location of the IP address for the computer distributing child pornography, Officer Watkins obtained a search warrant for the Weast residence in White Settlement.

When Officer Watkins executed a search warrant at the Weast residence, he seized a number of computers and electronic storage devices, including items from defendant Weast's bedroom. A forensic examination of devices located in Weast's bedroom revealed the presence of file-sharing software and child pornography. [a copy of the search warrant and affidavit, which describe the officer's method of downloading files are included in Exhibit A.]

Argument and authorities

A. Publicly available files are not protected by the Fourth Amendment

Weast now contends that, while he made files publicly available through his computer, law enforcement's access to those files encroached on his Fourth Amendment right to privacy.

To establish a Fourth Amendment violation, the defendant must show that he had "a reasonable expectation of privacy" in the property to be searched. *United States v. Setser*, 568 F.3d 482, 490 (5th Cir. 2009). That showing requires the defendant "to prove that he had (1) an actual, subjective expectation of privacy, and (2) that the expectation is one which society would recognize as reasonable." *Id.* at 490-91 (internal quotations, citation omitted); *see also*, *Katz v. United States*, 389 U.S. 347, 361 (1967) (concurring opinion). "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz*, 389 U.S. at 351. Therefore, in challenging an alleged "search" of his publicly shared computer folder, defendant bears the burden of establishing both a subjective and an objective expectation of privacy.

The Ninth Circuit has concluded a defendant has no reasonable expectation of privacy in files that he makes available through file sharing software. *United States v. Borowy*, 595 F.3d 1045, 1047 (9th Cir. 2010).

The Eleventh Circuit also rejected the argument that law enforcement improperly and unconstitutionally "electronically trespassed" on a defendant's property when it accessed the publicly shared folder of a defendant's computer. In *United States v. Norman*, 448 F. App'x 895 (11th Cir. 2011) (unpublished opinion)(copy attached), the defendant complained of the government's use of specialized software without a warrant to obtain information on his computer from the shared folder of a file-sharing program. *Id.* at 896. As a result, the defendant argued, the evidence subsequently seized during the execution of a search warrant at his residence was unlawfully obtained. *Id.*

The appellate court first recognized that Norman's act of placing the contents of his folder in the public domain negated any reasonable expectation of privacy in the folder. *Id.* at 897. Further, Norman's objection to law enforcement's use of "unique" software not available to the general public was "misplaced," because they acquired the same information he made available to the public. *Id.* Hence, Norman's motion to suppress was properly denied. *Id.*

Although the Fifth Circuit has not addressed this particular issue, one Western District of Texas court has arrived at a similar conclusion as the Eleventh Circuit in *Norman* and other circuits-- no reasonable expectation of privacy exists in files made publicly available through file-sharing programs. *United States v. Dodson*, 960 F.Supp.2d 689 (W.D. Texas 2013). *Dodson* is factually very similar to Weast's case. Dodson involved an agent using the Child Protection System (CPS) program to locate users sharing child pornography on file-sharing networks. *Id.* at 692. Investigation in that case began after the agent downloaded a child pornography file and sent a summons to AT&T to acquire the subscriber information associated with the IP address that was being used to share child pornography. *Id.* at 693. Law enforcement then obtained and executed a search warrant at the Dodson residence. *Id.* Dodson challenged use of the CPS software system as constituting a warrantless search of his computer; the district court disagreed. *Id.* at 694.

Once again, the court first examined (1) whether the defendant was able to establish an actual, subjective expectation of privacy with respect to the place being searched or the items being seized, and (2) whether that expectation of privacy was one

that society would recognize as reasonable. *Id.* (citing *United States v. Gomez*, 276 F.3d 694, 697 (5th Cir. 2001)). The court then concluded that the defendant had no expectation of privacy "because Defendant had already exposed the entirety of his files to the many unknown users" on the file-sharing network, "which is the exact opposite of exhibiting an expectation of privacy." *Id.* (also citing *United States v. Yang*, 478 F.3d 832, 835 (7th Cir. 2007)).

The district court also concluded that society would not willingly recognize an expectation of privacy where a user of file-sharing software had publicly shared files. *Id.* at 695. In support, the court relied on an unpublished decision out of the Northern District of Texas as well decisions from several other circuits.[3] *Id.*

Norman and *Dodson* are directly on point. Weast had no reasonable expectation of privacy in his Shareaza shared folder, which contained child pornography viewed by law enforcement. Using software available to law enforcement, Officer Watkins identified the defendant's computer as a likely distributor of child pornography. This identification was possible because the contents of Weast's shared folder on his computer were available to members of the public through the use of a peer-to-peer file sharing program. Moreover, the software Officer Watkins used did not search any areas of Weast's computer, download any files, or otherwise reveal any information that was unavailable to ordinary internet users.

---

[3] *United States v. Samples*, 2011 WL 4907315, *5 (N.D. Tex. Sept. 15, 2011) (Finding no ineffective assistance of counsel where counsel failed to challenge the use of forensic software to download files in a file-sharing case "because a user has no reasonable expectation of privacy in his public files"); *Borowy*, 595 F.3d at 1048; *United States v. Stults*, 575 F.3d 834, 842-45 (8th Cir. 2009); and *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008).

Accordingly, Weast cannot establish that he had a reasonable expectation of privacy in files that he made available to the public, and his claims of a Fourth Amendment violation must fail.

B. There is no reasonable expectation of privacy in subscriber information

Weast also contends that law enforcement's use of a subpoena to obtain subscriber information associated with his IP address violates the Fourth Amendment. Computers use IP addresses to communicate with each other, similar to the post office using a home address to deliver mail to a resident. There is no reasonable expectation of privacy in an IP address. *United States v. Christie*, 624 F.3d 558, 573 (3d Cir. 2010); *see also*, *Dodson*, 960 F.Supp.2d at 693, n.5).

The government is unclear as to what privacy expectation Weast asserts that he possessed in the subscriber information related to his *father's* internet account. But regardless, there is also no Fourth Amendment protection in customer accounts maintained by and for an Internet provider's business. "Subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation because it is voluntarily conveyed to third parties." *Christie*, 624 F.3d at 573; *see also*, *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) ("Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation.")[4]

[4] *Perrine* cites the following cases in support of its conclusion: *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001)(consistent holding in a non-criminal context); *United States v. Hambrick*, 225 F.3d 656 (4th Cir. 2000) (unpublished); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008); *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004).

In the *Perrine* case, the defendant, like Weast, used file-sharing software to make files available to the public through the Internet. The Tenth Circuit court found, "To the extent such access could expose his subscriber information to outsiders, that additionally vitiates any expectation of privacy he might have in his computer and its contents." *Perrine*, 518 F.3d 1205.

Riley v. California does not abrogate the holdings by these numerous courts that subscriber information is not protected by the Fourth Amendment. 134 S.Ct. 2473 (U.S. 2014). *Riley* involved two defendants whose cell phones were searched pursuant to their arrest. *Id.* at 2480-81. In those cases, the Fourth Amendment was triggered by the defendants' arrests, and the officers sought to search the cell phones pursuant to an exception to the warrant requirement—search incident to arrest. *Id.* at 2482.

Here, there was no "search" by the government to raise the protections of the Fourth Amendment. *See, Borowy*, 595 F.3d at 1047, ("Under *Katz*..., government conduct qualifies as a search only if it violates a reasonable expectation of privacy.")(internal citation omitted). Officer Watkins acquired publicly available child pornography files; his conduct did not amount to a search because Weast had no reasonable expectation of privacy in those files. Similarly, Weast has no reasonable expectation of privacy in the IP address and subscriber information voluntarily provided by Weast's father.

Therefore, the government respectfully requests the Court deny Weast's motion to suppress.

Respectfully submitted,

SARAH R. SALDAÑA
UNITED STATES ATTORNEY

AISHA SALEEM
Assistant United States Attorney
Texas State Bar No. 00786218
801 Cherry Street, Suite 1700
Fort Worth, Texas 76102
Telephone: 817-252-5200
Facsimile: 817-252-5455
Email: aisha.saleem@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on July 21, 2014, the foregoing Government's Response to Weast's Motion to Suppress was served by hand delivery to Angela Saad at 819 Taylor Street, Room 9A10, Fort Worth, Texas 76102.

AISHA SALEEM
Assistant United States Attorney

A

SEARCH WARRANT

THE STATE OF TEXAS
COUNTY OF TARRANT

To any Peace Officer of the State of Texas, **GREETINGS**:

WHEREAS, the Affiant whose name appears on the affidavit is a Peace Officer under the laws of Texas and did heretofore this day subscribe and swear to said Affidavit before me and whereas I find that the verified facts stated by Affiant in said Affidavit show that Affiant has probable cause for the belief expressed therein and establish the existence of proper grounds for issuance of this Warrant.

Now, therefore, you are commanded to enter the suspected place described as:

833 Hallvale Drive, White Settlement, Tarrant County, Texas 76108 is a one story, single family residence composed of red brick, white trim, and a brown composition shingle roof. There is a concrete driveway on the north side of the residence with a covered carport. The front door of the residence faces east. The numbers "833" are painted on the curb directly in front of the residence.

And to there search for, seize, conduct a forensic computer analysis and bring before me the personal property described below:

1. Any and all electronic devices that are capable of analyzing, creating, displaying, converting, or transmitting electronic or magnetic computer impulses or data that are used, owned, or accessed by **Christopher Robert Weast**, or any other person at this residence. These devices include but are not limited to: computers (including self-contained "laptop" or "notebook" computers), computer components, computer peripherals, word processing equipment, modems, monitors, printers, keyboards, acoustic couplers, cables, plotters, encryption circuit boards, optical scanners, external hard drives, digital cameras and other computer-related electronic or physical devices that serve to transmit or receive information to or from a computer.

2. Any and all information and/or data stored in the form of magnetic or electronic coding on a computer media or on media capable of being read by a computer or with the aid of computer-related equipment. This media includes, but in not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, zip disks, compact disk (CD) storage devices, tapes, laser disks, videocassettes, and any other media that is capable of storing magnetic coding.

3. Any and all instructions or programs stored in the form of electronic or magnetic media that are capable of being interpreted by a computer or related components. The items to be seized include but are not limited to: operating systems, application software (like word processing, graphics, or spreadsheet programs), utility programs, compilers, interpreters, communications programs, and any other programs or software used to communicate with computer hardware or peripherals either directly or indirectly via telephone lines, radio, or other means of transmission.

18-5-1008-18

4. Any documentation that proves ownership or maintenance of control of electronic or computer-related equipment, programs, data, or do information relating to same, including correspondence, invoices, computer printouts, and similar items.

5. Cellular telephones, automatic dialing devices, telephone answering machines, or any other electronic device used for the electronic storage of names, addresses, phone numbers, text messaging, e-mail or web access.

6. Any and all written or printed material that provides instructions or examples concerning the operation of a computer system, computer software, and/or any related device. Paper, documents or any other readable material, whether generated by handwriting, typewriter, computer, or any other device, which relates to Possession/Promotion of Child Pornography.

Further, you are ORDERED, pursuant to the provisions of Article 18.10, Texas Code of Criminal Procedure, to retain custody of any property seized pursuant to this Warrant, until further order of this Court or any other court of appropriate jurisdiction shall otherwise direct the manner of safekeeping of said property. This Court grants you leave and authority to remove such seized property from this county, if and only if such removal is necessary for the safekeeping of such seized property by you, or if the provisions of Article 18.10, T.C.C.P. otherwise authorize such removal. You are further ORDERED to give notice to this Court, as a part of the inventory to be filed subsequent to the execution of this Warrant, and as required by Article 18.10, T.C.C.P., of the place where the property seized hereunder is kept, stored and held.

HEREIN FAIL NOT, but have you then and there this Warrant within three days, exclusive of the day of its issuance and exclusive of the day of its execution, with your return thereon, showing how you executed the same, file in this court.

ISSUED THIS THE 10 day of July, A.D., 2012, at 02:21 o'clock A.M. to certify which witness my hand this day.

MAGISTRATE/JUDGE
Judge, City of Ft. Worth

MUNICIPAL COURT OF FORT WORTH, TEXAS

12-S-1008-12

SEARCH WARRANT AFFIDAVIT

THE STATE OF TEXAS
COUNTY OF TARRANT

THE UNDERSIGNED AFFIANT, BEING A PEACE OFFICER UNDER THE LAWS OF TEXAS AND BEING DULY SWORN, ON OATH MAKES THE FOLLOWING STATEMENTS AND ACCUSATIONS.

THERE IS IN TARRANT COUNTY, TEXAS, A SUSPECTED PLACE DESCRIBED AND LOCATED AS FOLLOWS:

833 Hallvale Drive, White Settlement, Tarrant County, Texas 76108 is a one story, single family residence composed of red brick, white trim, and a brown composition shingle roof. There is a concrete driveway on the north side of the residence with a covered carport. The front door of the residence faces east. The numbers "833" are painted on the curb directly in front of the residence.

IT IS THE BELIEF OF AFFIANT THAT AT THE SUSPECTED PLACE THERE WILL BE FOUND PROPERTY AND ITEMS CONSTITUTING CONTRABAND AND INSTRUMENTS USED TO COMMIT CRIMINAL ACTS IN VIOLATION OF THE LAWS OF TEXAS. SUCH PROPERTY AND ITEMS WILL CONSIST OF THE FOLLOWING:

1. Any and all electronic devices that are capable of analyzing, creating, displaying, converting, or transmitting electronic or magnetic computer impulses or data that are used, owned, or accessed by **Christopher Robert Weast,** or any other person at this residence. These devices include but are not limited to: computers (including self-contained "laptop" or "notebook" computers), computer components, computer peripherals, word processing equipment, modems, monitors, printers, keyboards, acoustic couplers, cables, plotters, encryption circuit boards, optical scanners, external hard drives, digital cameras and other computer-related electronic or physical devices that serve to transmit or receive information to or from a computer.

2. Any and all information and/or data stored in the form of magnetic or electronic coding on a computer media or on media capable of being read by a computer or with the aid of computer-related equipment. This media includes, but in not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, zip disks, compact disk (CD) storage devices, tapes, laser disks, videocassettes, and any other media that is capable of storing magnetic coding.

3. Any and all instructions or programs stored in the form of electronic or magnetic media that are capable of being interpreted by a computer or related components. The items to be seized include but are not limited to: operating systems, application software (like word processing, graphics, or spreadsheet programs), utility programs, compilers, interpreters, communications programs, and any other programs or software used to communicate with computer hardware or peripherals either directly or indirectly via telephone lines, radio, or other means of transmission.

12-S-1008-12

4. Any documentation that proves ownership or maintenance of control of electronic or computer-related equipment, programs, data, or do information relating to same, including correspondence, invoices, computer printouts, and similar items.

5. Cellular telephones, automatic dialing devices, telephone answering machines, or any other electronic device used for the electronic storage of names, addresses, phone numbers, text messaging, e-mail or web access.

6. Any and all written or printed material that provides instructions or examples concerning the operation of a computer system, computer software, and/or any related device. Paper, documents or any other readable material, whether generated by handwriting, typewriter, computer, or any other device, which relates to Possession/Promotion of Child Pornography.

A. OVERVIEW OF PEER-TO-PEER CHILD PORNOGRAPHY INVESTIGATION TERMS, BACKGROUND AND METHODOLOGY:

1. This investigation was initiated as a result of the law enforcement community's ongoing concern related to the escalating prevalence of the distribution of child pornography via "Peer to Peer" (P2P) file sharing software. P2P file sharing programs are a standard way of transferring files from one computer system to another while connected to the Internet. P2P file sharing programs allow groups of computers using the same file sharing network, e.g. "Gnutella" to connect directly with each other and to share files from one another's computer systems. Presently, millions of persons throughout the world use P2P file sharing networks to share many types of files among each other. P2P application software allows networked computer users, connected to the Internet, to share many types of files with other users. These files typically include music, graphics, images, movies, and text. In this way, users are able to collect large numbers of files, including child pornography.

2. The most prevalent P2P file sharing network presently in use today is known as the "Gnutella Network". Gnutella is a system that allows individuals to use their computers to exchange files directly over the Internet without having to go through or access a specific Web site in an arrangement that can be described as computer to computer (or person to person, hence the name "Peer to Peer"). Unlike a Web site, Gnutella enables person to obtain files directly from one another as long as they are connected to the Internet. Furthermore, Gnutella enables an individual to view the files made available to share to other Gnutella users. Upon installation and enabling of Gnutella on one's computer, that computer then becomes both a client and a server in the network and is able to share desired files that have been placed in what is referred to as a "shared folder" on a user's hard drive, with other Gnutella users. The Gnutella network is presently utilized by numerous Peer-to-Peer file sharing programs, including, but not limited to "Limewire", "Frostwire", and "Bearshare". These aforementioned programs connected to the Gnutella network have software installed on them that facilitates the trading of images and other files. The software, when installed, allows the user to search for pictures, movies, and other digital files by entering text as search terms. For example, an individual looking for music files by a specific artist may enter a search term such as "Eagles" and will receive nearly instantaneously a list of other Gnutella users that have music titles pertaining to

12-S-1008-12

music artist "The Eagles" on their hard drives that have been made available to others on the network.

3. Because of its relative ease of use and perceived anonymity, P2P networks provide readily available access to child pornography. As a result, beginning in November 2004, law enforcement officers throughout the United States have participated in an Internet undercover operation to identify persons using the Gnutella peer to peer software on the Internet to traffic in child pornography. These law enforcement officers knew from using the Gnutella network that users can find images and movies of child pornography by using search terms like "babyj". The "babyj" search term typically results in the user being presented with a listing of files that include movies of a known child from Georgia being penetrated vaginally by an adult male. The files associated with "babyj" often refer to the series of child pornography videos previously identified in another investigation.

4. It is known from using the Gnutella network software that the search results presented to the user allow the user to select a file and then receive that file from the other users around the world. Often these users can receive the selected movie from the numerous sources at once. The software can balance the network load and recover from the network failures by accepting pieces of the movie from different users and then reassembling the movie on the local computer.

5. Your Affiant knows that the Gnutella network can only succeed in reassembling the movie from different parts if the parts all come from the exact same movie. Your Affiant knows that multiple persons sharing one movie can deliver different pieces of that movie to the local software and the local software can insure a complete and exact copy can be made from the parts. Officers have been able to confirm from the use of the software that the different copies of the same movie may have different file names.

6. Your Affiant knows that computer software has different methods to insure that two files are exactly the same. Your Affiant knows that the method used by the Gnutella network involves a file encryption method called Secure Hash Algorithm (SHA), developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), for the use with the Digital Signature Standard (DSS) is specific within the Secure Hash Standard (SHS). The United States of America has adopted the SHA-1 has algorithm described herein as a Federal Information Processing Standard.

7. Your Affiant knows that the digital files can be processed by this SHA-1 process resulting in a digital signature, akin to a fingerprint. By comparing these digital signatures one can conclude that two files are identical with a precision that greatly exceeds 99.9999 percent certainty. Your Affiant is aware that law enforcement officers have researched the work of many in the computer forensics community and have been unable to locate any documented occurrence of two different files having different contents while having the same SHA-1 value.

12-5-1008-12

8. During the course of this investigation, officers have learned from using the Gnutella software that the system uses the SHA-1 digital signature to verify the unique identity of individual files. Pursuant to this investigation, your Affiant has been able to demonstrate that users attempting to trade files on the Gnutella file-sharing network can choose to place files from their local computer into a shared file directory available via the network. If that same user then starts the Gnutella software, that local computer could then calculate the SHA-1 signature for each shared file and provide that information to other users wishing to trade files.

9. Pursuant to this investigation, your Affiant has learned that entering a query in the Gnutella network software results in a list of SHA-1 digital signatures that can then be viewed. By querying the Gnutella network, your Affiant can compare the offered SHA-1 signatures with SHA-1 signatures that belong to movies or images of known or suspected child pornography. These known or suspected movies or images of child pornography have been compiled by law enforcement agencies during the course of separate and unrelated Internet child sexual exploitation investigations into a database readily accessible for law enforcement use. Once a matching set of digital signatures is identified, your Affiant then uses publicly available software to request a list of network computers/users that are reported to have the same images available for distribution. This process allows your Affiant to identify known or suspected images of child pornography, including movie files that are publicly available on the Gnutella network.

10. Your Affiant knows from training and experience that Internet computers identify each other by an Internet Protocol or IP address. Your Affiant knows that these IP addresses can assist law enforcement in finding a particular computer on the Internet. These IP addresses can typically lead the law enforcement officer to a particular Internet service provider company and that company can typically identify the account that uses the IP address to access the Internet.

11. Your Affiant has been able to capitalize on the Internet's and Gnutella network's reliance on IP addresses to geographically locate computers within or near the City of Fort Worth that have made known images and/or movies of child pornography available for distribution via Peer to Peer file sharing. This specificity to a geographic location via IP address has been made possible through the utilization of software developed by Flint Waters, formerly a Special Agent with the Wyoming Division of Criminal Investigations, which enables investigators to categorize IP addresses by geographical parameters.

12. Your Affiant learned that querying the Gnutella peer to peer network as described can result in him receiving a list of IP addresses identifying locations where a computer has Gnutella software installed and individual files have been reported as available for download with a specific digital signature (SHA-1). Your Affiant then utilizes Flint Waters' software to examine the list of IP addresses to locate computers that are suspected to be somewhere within the approximate geographic range of the City of Fort Worth. By comparison of the SHA-1 digital signatures one can conclude that a computer, originating from an IP address known to be within or near the City of Fort Worth, which through further investigation is subsequently pinpointed to a specific location, has Gnutella or compatible software installed on it and contains known or suspected images of child pornography.

12-S-1008-12

13. It should be noted that the software developed by Flint Waters merely categorizes by general geography IP addresses that have been broadcast by a suspect's own computer onto the network as a function of the network software. Because the software developed by Flint Waters does not provide any additional identifying data other than a user's IP address, it is incumbent upon investigating officers to take additional steps toward the identification and specific location of the computer that is being utilized to distribute child pornography. The ability to view the file names and SHA-1 values a suspect has on his computer is a direct function of the Peer to Peer file sharing software that the suspect has freely and independently utilized in furtherance of his file sharing activities, and is not a function of any software designed by or proprietarily utilized by law enforcement. Simply stated, by definition the suspect himself has in effect advertised publicly, via the Internet, which files he has on his hard drive by making those files available to Gnutella network users. Law enforcement officers have simply availed themselves of this information by accessing the Gnutella network in the same fashion that any private individual is able to do.

14. Based on the foregoing, you Affiant, along with other participating law enforcement agencies, initiated an investigation concentrating on the identification of computers and persons located within or near the City of Fort Worth that are distributing images and/or movie files of child pornography via the Internet through the utilization of Peer to Peer file sharing software.

B. AFFIANT HAS PROBABLE CAUSE FOR THE SAID BELIEF BY REASON OF THE FOLLOWING FACTS, TO WIT:

Affiant, Officer Randy D. Watkins #3439, is a certified and licensed Texas Peace Officer with more than twenty years of law enforcement experience. Affiant is currently assigned to the Crimes Against Children Unit of the Fort Worth Police Department, and has focused on crimes involving the use of computers and child exploitation.

Affiant has specialized training in the investigation of crimes committed through the use of the Internet. Among course work completed by Affiant are:

- Computer Crimes Investigation School, Texas DPS, Austin, Texas
- Basic Data Recovery and Analysis, Dallas Texas
- NIPC 101, FBI, Dallas, Texas
- Criminal Investigations, TCJC Northwest Campus, Ft. Worth, Texas
- Advanced Criminal Investigations, NTCOG, Arlington, Texas
- Basic and Advanced Reid Interview/Interrogations, Austin, Texas
- SEARCH Online Investigations School, Austin, Texas
- Possesses an Advanced TCLEOSE peace officer license
- Basic Child Abuse Investigations
- ICAC Peer Precision Training Technical Assistance, Irving, Texas
- Project Safe Childhood Team Training, Houston, Texas
- Sex Crimes and Homicide Analysis, Fort Worth, Texas
- Analytical Investigative Techniques, Irving, Texas
- SEARCH Peer to Peer Investigations, Boca Raton, Florida
- Internet and Technology facilitated sexual exploitation of children, Boca Raton, Florida

12-S-1008-12

On 6/4/12, the Affiant, Officer R.D. Watkins #3439, of the Fort Worth Police Department, Crimes Against Children Unit, was investigating the promotion of child pornography on the Internet. The Affiant has been trained and is authorized in this capacity by "Operation Fair Play". "Operation Fair Play" provides training to local law enforcement on how to investigate these child exploitation crimes.

On 6/4/12 at approximately 1420 hours, using a program called the Child Protection System, the Affiant located an Internet Protocol (IP) address that was offering to participate in the Promotion of Child Pornography. The IP address was 99.71.201.174. The suspect IP address was offering to share files via the Internet on the Gnutella Network. Using the Child Protection System program, the Affiant could see under the "Unique Files" section that the suspect IP address had 3543 categorized files and that 1761 of those files were "Child Notable" (images and/or videos of known child pornography). The Child Protection System program compares the SHA values of the images and/or videos against a database of SHA files that law enforcement officers have looked at and believe to contain suspected or known child pornography. ** SHA is Secure Hash Algorithm, similar to an electronic fingerprint for files. The chance of two files having the same SHA and different content is astronomical.

Using an additional program called ShareazaLE, the Affiant attempted to download these "child notable" files from the suspect IP address. As ShareazaLE was downloading the files from IP 99.71.201.174, the Affiant noticed in the log files that the computer nickname being downloaded from was named "Chris".

The downloaded images/videos were automatically stored in a download file under the IP address of 99.71.201.174. The first download took place on 6/4/12 at 14:21 local time. Adding 5 hours to the local time, this converts to 19:21 GMT. The following is a description of some of the photographs downloaded from the suspect IP:

Photograph titled: "Imgsrc Ru pthc Pdeo Babyshivid Childlover Private Daughter Torpedo Ranchi Lolita - 1596344.jpg" and is of a white female approximately 5-6 years of age, completely nude performing oral sex on an adult white male.

Photograph titled: "Private Daughter Mellony Stolen Pedo Lolita Pthc Hussyfan Preteen Nude (10Yo) 18.jpg" and is of a white female approximately 8-10 years of age, lying on her back, appears to be completely nude, with her legs spread exposing her vagina.

Photograph titled: "Private Daughter Mellony Stolen Pedo Lolita Pthc Hussyfan Preteen Nude (10Yo) 56.jpg" and is of a white female approximately 8-10 years of age, lying on her back, completely nude, with her legs spread exposing her vagina.

Photograph titled: "!!!!! 2006 older man fuckt little boy kolja 10yo pthc kdv ass preteen nice hot (35).jpg" and is of a white male approximately 9-10 years of age performing oral sex on an adult white males erect penis.

Photograph titled: "Anita 14yo gives her uncle a nice blowjob reelkiddymov child Lolita hardcore pedo fuck small porn kiddy(1)(1)(1).jpg" and is of a white female approximately 10-12 years of age, completely nude, performing oral sex on what appears to be an adult white males erect penis.

12-S-1008-12

Photograph titled: "Kopie Von Kopie Von -ImgsrcRu New Users New Photos New Girls Pthc Pedo 12Yo 11Yo 1Yo 9Yo 8 Yo 7Yo 6Yo 0024 0.jpg" and is of two white females approximately 7-8 years of age, both appear to be completely nude, with an adult male that is nude except for white socks. One of the females is kissing the adult male while the other is performing oral sex on his erect penis.

A total of 66 images of child pornography or suspected child pornography have been downloaded from the suspect IP address to this point.

The suspect IP address was checked using centralops.net and found to be owned by SBC Internet Services, Inc.

On 6/6/12 using this information, the Affiant prepared a subpoena request for account information on who was assigned IP address 99.71.201.174 on 6/4/12 at 19:21 GMT (1421 hours central time). The subpoena request was sent to the Tarrant County District Attorney's Office for processing.

On 6/20/12, the Affiant received the subpoena return from SBC Internet Services with account information on who/what account was assigned Internet Protocol (IP) address 99.71.201.174 on Monday, June 4, 2012 at 19:21 GMT. The SBC Internet Services subpoena return showed that on this date and time that IP address was assigned to account #116103070, Larry Weast, telephone #817-246-3866, 833 Hallvale Drive, White Settlement, Texas 76108.

A check of TLO, a database available to law enforcement that searches public records, revealed that a Christopher Robert Weast, white male, date of birth 01/31/74, Texas driver's license 15977594, social security 636-03-1074, is associated with Larry Weast at 833 Hallvale Drive, White Settlement, Texas 76108. This is significant because the download logs from this case show the downloads not only coming from IP address 99.71.201.174, but from a computer nicknamed "Chris".

C. THE FOLLOWING CONSIDERATIONS AND PRACTICALITIES GOVERN THE MANNER OF THE EXECUTION OF THE SEARCH WARRANT:

Based upon Affiant's knowledge, training, and experience, and experience of other law enforcement personnel, Affiant knows that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, all computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, must be seized and subsequently processed by a qualified computer specialist in an appropriate setting. Accordingly, it is very often necessary to take all computer hardware and software found at the suspected location in order to have it examined in a qualified forensic environment. Such will sometimes be the only way that items such as previously sent and received e-mails can be effectively recovered from a computer or its password, can be encrypted, or could have been previously "deleted." In light of these concerns, Affiant requests the Court's permission to seize at the search location all the computer hardware, software, and peripherals that are believed to potentially contain some or all of the contraband, or instrumentalities described in the warrant, and to have a forensic search of these computer materials conducted for such evidence. Affiant intends to transport some computer materials to a qualified forensic facility for imaging and analysis by experts. The storage of such material can be for months and even years, and such persons are sometimes not even aware that the storage occurs, due to that even "deleted" items can be recovered from the hard drive. Indeed, since the mid 1990s the computer has become the ideal

12-S-1008-12

mechanism for storing such material, insofar as a computer can hold hundreds or thousands of images and text documents in a compact space hidden from sight, protected from the eyes of others, but nonetheless easily retrievable by the user.

WHEREFORE, AFFIANT ASKS FOR ISSUANCE OF A WARRANT THAT WILL AUTHORIZE THE SEARCH OF SAID SUSPECTED PLACE FOR SAID PERSONAL PROPERTY AND SEIZURE OF THE SAME (INCLUDING THE COMPUTER HARDWARE HOUSING IT) AND TO CONDUCT A FORENSIC COMPUTER EXAMINATION OF SAID SEIZED PROPERTY.

D Watt 3439
AFFIANT

SUBSCRIBED AND SWORN TO BEFORE ME BY SAID AFFIANT ON THE 10 DAY OF July, A.D., 2012.

MAGISTRATE
JUDGE, City of Ft. Worth

MUNICIPAL COURT OF FORT WORTH, TEXAS

12-5-1008-12

THE STATE OF TEXAS
COUNTY OF TARRANT

SEARCH WARRANT RETURN
12-S-1008-12

On July 10, 2012, your Affiant, Officer R.D. Watkins #3439, assigned to the Fort Worth Police Department, Crimes Against Children Unit, executed the above search warrant for the offense of Promotion of Child Pornography and seized the following items:

- One Dell computer with built in monitor and thumb drive, Serial #TB78KMPTT2DXD7FQK
- One HP, Pavilion, entertainment, laptop computer, Serial #CNF8234HX7
- One black, external hard drive, Serial #WCAV5C309672
- One Mac Mini 2 external hard drive with Microsoft thumb drive, Serial #YMB240GEYL2
- One black, Toshiba, CPU, Serial #057011254D
- One Sony Vaio CPU, model #PCV-7753, Serial #284445303001493
- One Sony Vaio CPU, model #PCV-C12L, Serial #STR4669144
- One Western Digital, hard drive, Serial #WM9070276587
- One Samsung, hard drive, Serial #0400J1FT512028
- One Seagate, hard drive, Serial #5LRBFTPZ
- One Quantum, Fireball, hard drive, Serial #693931231765
- Six DVD/CD's

Witness my signature, this the 16 day of July, 2012.

R D Watkins 3439
Affiant

Subscribed and sworn to before me on this the 16 day of July, 2012, at 2:06 o'clock S .m.

Magistrate

MUNICIPAL COURT OF FORT WORTH, TEXAS

B

Westlaw.

448 Fed.Appx. 895, 2011 WL 4551570 (C.A.11 (Ala.))
(Not Selected for publication in the Federal Reporter)
(Cite as: 448 Fed.Appx. 895, 2011 WL 4551570 (C.A.11 (Ala.)))

H

This case was not selected for publication in the Federal Reporter.

Not for Publication in West's Federal Reporter See Fed. Rule of Appellate Procedure 32.1 generally governing citation of judicial decisions issued on or after Jan. 1, 2007. See also Eleventh Circuit Rules 36-2, 36-3. (Find CTA11 Rule 36-2 and Find CTA11 Rule 36-3)

United States Court of Appeals,
Eleventh Circuit.
UNITED STATES of America, Plaintiff–Appellee,
v.
David Waterman NORMAN, Jr., Defendant–Appellant.

No. 11–11046
Non–Argument Calendar.
Oct. 4, 2011.

Background: After the United States District Court for the Middle District of Alabama, 2:09–cr–00118–WKW–CSC–1, 2010 WL 3825601, denied defendant's motion to suppress evidence, he was convicted by jury of knowingly possessing child pornography on an external hard drive. He appealed denial of motion to suppress.

Holdings: The Court of Appeals held that:
(1) defendant did not have an objectively reasonable expectation of privacy in shared files on his computer, and
(2) sufficient evidence supported jury's finding that defendant knowingly possessed child pornography on an external hard drive.

Affirmed.

West Headnotes

[1] Obscenity 281 ⇐274(2)

281 Obscenity
281VI Searches and Seizures
281k272 Warrantless Searches
281k274 Expectation of Privacy
281k274(2) k. Computers; electronic transmission. Most Cited Cases
(Formerly 281k7.6)

Even if defendant convicted of knowingly possessing child pornography held a subjectively reasonable expectation of privacy in shared files on his computer, this expectation was not objectively reasonable where his computer contained a peer-to-peer file-sharing program that allowed other public users of such software to access the shared files on his computer, and thus police officers' warrantless access and search of the shared files did not violate Fourth Amendment. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 2252A(a)(5)(B).

[2] Obscenity 281 ⇐210(12)

281 Obscenity
281IV Prosecution
281k206 Evidence
281k210 Weight and Sufficiency
281k210(9) Depiction of Minors; Child Pornography
281k210(12) k. Possession. Most Cited Cases
(Formerly 281k17)

Sufficient evidence supported jury's finding that defendant knowingly possessed child pornography on an external hard drive, including defendant's admission to police that they would "absolutely" find child pornography on his computer, testimony of witnesses that established that defendant had purchased the external hard drive, the hard drive was located in his bedroom, and that hard drive had same 62 files of child pornography which had been transferred from his computer to the hard drive, and testimony from defendant's son that he had not transferred pornographic files from his laptop or from his father's computer to the external hard drive. 18 U.S.C.A. § 2252A(a)(5)(B).

448 Fed.Appx. 895, 2011 WL 4551570 (C.A.11 (Ala.))
(Not Selected for publication in the Federal Reporter)
(Cite as: 448 Fed.Appx. 895, 2011 WL 4551570 (C.A.11 (Ala.)))

***896** Leura Garrett Canary, Nathan D. Stump, U.S. Attorney's Office, Montgomery, AL, for Plaintiff–Appellee.

Christine A. Freeman, Federal Defender Program, Inc., Montgomery, AL, for Defendant–Appellant.

Appeal from the United States District Court for the Middle District of Alabama. D.C. Docket No. 2:09–cr–00118–WKW–CSC–1.

Before MARCUS, WILSON and BLACK, Circuit Judges.

PER CURIAM:

****1** David Waterman Norman Jr. appeals from his conviction for knowingly possessing child pornography on an external hard drive, in violation of 18 U.S.C. § 2252A(a)(5)(B). On appeal, Norman argues that: (1) the government used specialized computer software to obtain information from the shared-files folder of his computer without a warrant, and that the evidence subsequently seized during the execution of a search warrant at his residence was unlawfully obtained and should have been excluded from trial; and (2) the government failed to present any evidence that he knowingly downloaded or saved child pornography because the evidence established that multiple people used the computer in his bedroom and that at least one child pornography file was copied to the external hard drive at issue from the folder of one of Norman's sons. After careful review, we affirm.

Our review of the denial of a motion to suppress is a mixed question of law and fact, with rulings of law reviewed *de novo* and findings of fact reviewed for clear error. *United States v. Lanzon,* 639 F.3d 1293, 1299 (11th Cir.2011), *petition for cert. denied,* —— U.S. ——, 132 S.Ct. 333, 181 L.Ed.2d 208, 2011 WL 4536264 (2011). Findings of fact are viewed in the light most favorable to the prevailing party in the district court. *Id.* We review " *de novo* whether sufficient evidence supports a conviction, resolving all reasonable inferences in favor of the verdict." *United States v. Farley,* 607 F.3d 1294, 1333 (11th Cir.), *cert. denied,* —— U.S. ——, 131 S.Ct. 369, 178 L.Ed.2d 238 (2010). "We will not reverse unless no reasonable trier of fact could find guilt beyond a reasonable doubt." *Id.* "It is not our function to make credibility choices or to pass upon the ***897** weight of the evidence. Instead, we must sustain the verdict where there is a reasonable basis in the record for it." *Id.* (quotations and citation omitted).

First, we are unpersuaded by Norman's claim that the district court erred in denying his motion to suppress. In order to challenge a search under the Fourth Amendment, the defendant bears the burden of establishing both a subjective and an objective expectation of privacy in the area or object searched. *United States v. Segura–Baltazar,* 448 F.3d 1281, 1286 (11th Cir.2006). "The subjective component requires that a person exhibit an actual expectation of privacy, while the objective component requires that the privacy expectation be one that society is prepared to recognize as reasonable." *United States v. Epps,* 613 F.3d 1093, 1097–98 (11th Cir.2010) (quotation omitted), *cert. denied,* —— U.S. ——, 131 S.Ct. 1526, 179 L.Ed.2d 344 (2011).

[1] Here, even if Norman held a subjectively reasonable expectation of privacy in the shared files on his computer, this expectation was not objectively reasonable. As the record shows, Norman's computer contained a peer-to-peer file-sharing program—which Norman himself used-that allowed other public users of such software to access the shared files on his computer. Moreover, Norman's argument that law enforcement used "unique" software that was not available to the general public, and his reliance on *Kyllo v. United States,* 533 U.S. 27, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001), are misplaced because, as noted, he had placed the contents of the folder the police searched into the public domain, thereby negating any reasonable expectation of privacy in the folder. In *Kyllo,* law enforcement used a thermal imager to scan the home of a

448 Fed.Appx. 895, 2011 WL 4551570 (C.A.11 (Ala.))
(Not Selected for publication in the Federal Reporter)
(Cite as: 448 Fed.Appx. 895, 2011 WL 4551570 (C.A.11 (Ala.)))

suspected marijuana grower to determine whether his home was emitting heat consistent with the use of high-intensity lamps for growing marijuana. 533 U.S. at 29–30, 121 S.Ct. 2038. The Supreme Court held that when the government uses a device, in that case a sense-enhancing thermal imager, which was not in general public use, to obtain information about the interior of a home that could not otherwise have been obtained without physical intrusion, the surveillance constitutes a search. *Id.* at 34, 40, 121 S.Ct. 2038. However, unlike in *Kyllo,* the contents of the shared folder on Norman's computer were knowable to law enforcement without physical intrusion to Norman's house because this information was also available to members of the public. Accordingly, Norman did not suffer a Fourth Amendment violation, and thus, the district court did not err in denying his motion to suppress.

****2** [2] We also find no merit in his sufficiency of the evidence claim. Pursuant to 18 U.S.C. § 2252A(a)(5)(B), it is unlawful to knowingly possess any material that contains an image of child pornography that has been mailed, shipped, or transported in interstate commerce. It is the duty of the trier of fact to "resolve conflicts in the testimony, to weigh the evidence, and to draw reasonable inferences from basic facts to ultimate facts," and we should only inquire as to whether " *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *Jackson v. Virginia,* 443 U.S. 307, 318–19, 99 S.Ct. 2781, 61 L.Ed.2d 560 (1979).

In this case, the only issue with respect to the sufficiency of the evidence established at trial is whether Norman knowingly possessed the images of child pornography on the external hard drive. The record reflects that there was sufficient evidence to permit the jury to find Norman guilty beyond a reasonable doubt of knowingly possessing these images on the external hard drive. Specifically, the evidence, ***898** viewed in the light most favorable to the government as to Count 2, established that: (1) Norman purchased the external hard drive and it was located in his bedroom; (2) the computer and external hard drive in Norman's bedroom contained the same files of child pornography—a total of 62—which had been transferred from the computer to the hard drive on two occasions; (3) on the two occasions that files containing child pornography were transferred from the computer to the external hard drive, Norman was not at work; (4) of the other witnesses who had access to the computer in Norman's bedroom, only Norman's son knew a hard drive was located there; (5) his son may have "plugged" the external hard drive into the computer in Norman's bedroom on one occasion; and (6) his son did not use Norman's computer to download child pornography, and did not transfer files from his laptop, or his father's computer, to the external hard drive. Indeed, the jury was entitled to believe the witnesses who testified that they did not place child pornography on the computer in Norman's bedroom. *Jackson,* 443 U.S. at 319, 99 S.Ct. 2781.

Importantly, when the police questioned Norman during the execution of the search warrant, he initially denied having any contact with child pornography, yet then not only admitted that he was "curious" about children, but also admitted that police would "[a]bsolutely" find child pornography on his computer. So although the questions the police officer asked did not address whether Norman knew child pornography was on the external hard drive, Norman's admissions, together with the other circumstantial evidence discussed above, were sufficient evidence for a rational juror to find Norman guilty beyond a reasonable doubt of knowingly possessing child pornography on the external hard drive. *See id.* Accordingly, we affirm his conviction.

AFFIRMED.

C.A.11 (Ala.),2011.
U.S. v. Norman
448 Fed.Appx. 895, 2011 WL 4551570 (C.A.11 (Ala.))

448 Fed.Appx. 895, 2011 WL 4551570 (C.A.11 (Ala.))
(Not Selected for publication in the Federal Reporter)
(Cite as: 448 Fed.Appx. 895, 2011 WL 4551570 (C.A.11 (Ala.)))

END OF DOCUMENT